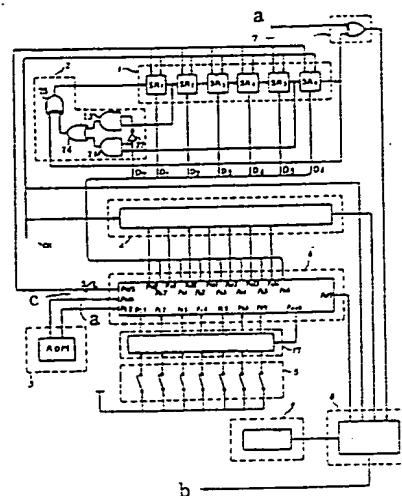


(54) **PRIVACY CALL EQUIPMENT**

(11) 3-76447 (A) (43) 2.4.1991 (19) JP
(21) Appl. No. 64-212613 (22) 18.8.1989
(71) SHARP CORP (72) JUNJI HIRAIDE(1)
(51) Int. Cl.³ H04L9/06, H04L9/14

PURPOSE: To sufficiently ensure the secrecy of communication by providing a conversion circuit revising a setting value of a cryptographic key from a cryptographic key setting means so as to revise the cryptographic key differently from each communication thereby revising the setting of the cryptographic key without disturbing the user.

CONSTITUTION: A cryptographic key from a cryptographic key setting means 5 is fed to a microcomputer 6 via a cryptographic key conversion circuit 17 comprising an arithmetic circuit. A data of number of times of communication is fed to the conversion circuit 17 from the microcomputer 6 and the cryptographic key supplied from the cryptographic key setting means 5 is revised to be different from each communication. Thus, it is not required to enter a decoding key at a receiver side and a sender side freely revises the cryptographic key. Then the cryptographic key from the cryptographic key setting means 5 is revised by the conversion circuit 17 different from each communication. Thus, the secrecy of the communication is sufficiently secured without disturbing the user.



CK: clock. a: data. c: address. b: communication line.
20: pseudo random signal generating circuit. 4: parallel serial conversion. 10: serial/parallel conversion. 3: storage circuit.
9: synchronizing signal generation circuit. 8: data control signal switching circuit. 7: cryptographic circuit

201 AVAILABLE COPY

THIS PAGE BLANK (USPTO)

⑨ 日本国特許庁(JP)

⑩ 特許出願公開

⑫ 公開特許公報(A)

平3-76447

⑤ Int. Cl.⁵

識別記号

庁内整理番号

⑬ 公開 平成3年(1991)4月2日

H 04 L 9/06
9/14

6914-5K H 04 L 9/02

Z

審査請求 未請求 請求項の数 1 (全6頁)

⑭ 発明の名称 秘話装置

⑮ 特 願 平1-212613

⑯ 出 願 平1(1989)8月18日

⑰ 発 明 者 平 出 順 二 大阪府大阪市阿倍野区長池町22番22号 シャープ株式会社
内

⑱ 発 明 者 多 田 順 次 大阪府大阪市阿倍野区長池町22番22号 シャープ株式会社
内

⑲ 出 願 人 シャープ株式会社 大阪府大阪市阿倍野区長池町22番22号

⑳ 代 理 人 弁理士 山口 邦夫

BEST AVAILABLE COPY

明 細 書

1. 発明の名称

秘 話 装 置

2. 特許請求の範囲

(1) 送信側には、

第1の疑似ランダム信号発生回路と、

暗号鍵を設定する暗号鍵設定手段と、

上記暗号鍵の設定値を変更する変換回路と、

上記疑似ランダム信号発生回路の初期設定データを記憶した第1の記憶回路と、

上記変換回路からの暗号鍵に対応したアドレス信号によって上記第1の記憶回路から上記初期設定データを読み出して上記第1の疑似ランダム信号発生回路を設定する第1の制御手段と、

上記第1の疑似ランダム信号発生回路の出力信号によって入力データを暗号化する暗号化回路とが備えられ、

上記暗号化回路の出力データおよび上記アドレス信号が送信され、

受信側には、

上記第1の疑似ランダム信号発生回路と同じ構成の第2の疑似ランダム信号発生回路と、

上記第1の記憶回路と同じ内容を記憶した第2の記憶回路と、

受信した上記アドレス信号によって上記第2の記憶回路から上記初期設定データを読み出して上記第2の疑似ランダム信号発生回路を設定する第2の制御手段と、

上記第2の疑似ランダム信号発生回路の出力信号によって受信したデータを復号化する復号化回路とが備えられることを特徴とする秘話装置。

3. 発明の詳細な説明

〔産業上の利用分野〕

この発明は、例えば有線あるいは無線ディジタル通信に使用して好適な秘話装置に関する。

〔従来の技術〕

通信において、通信内容が秘密である場合には秘話通信を行なう必要がある。この場合、送信側

では、通常データ(平文)が暗号化され、この暗号化データ(暗号文)が送信される。そして、受信側では、この暗号文が平文に復号化される。

第5図は、従来の秘密装置を示している。

同図において、送信側では、平文が暗号化回路13に供給されて暗号鍵に応じて暗号文に変換される。この暗号化回路13からの暗号文は、有線または無線の通信区間を介して、受信側に供給される。また、受信側では、暗号文が復号化回路14に供給されて復号化鍵16に応じて平文に変換される。

[発明が解決しようとする課題]

第5図例によれば、送信側および受信側が、暗号化および復号化のために、例えば同一の鍵を所有する必要がある。そのため、送信側では暗号鍵を自由に更新することができなかった。しかし、通信の秘密を確保するには、暗号鍵を度々更新する必要がある。

そこで、本出願人は、先に、暗号鍵を自由に変更できる秘密装置を提案した(特願平1-702

ータD7が供給される。また、アンドゲート23にはシフトレジスタSR1の出力信号が供給されると共に、制御データD7がインバータ22を介して供給される。そして、これらアンドゲート21および23の出力信号がオアゲート24に供給される。したがって、制御データD7がハイレベルかローレベルかに応じて、オアゲート24からはシフトレジスタSR1またはSR5の出力信号が出力される。

また、エクスクルーシブオアゲート25にはオアゲート24の出力信号が供給されると共に、シフトレジスタSR6の出力信号が供給される。そして、このエクスクルーシブオアゲート25の出力信号はシフトレジスタSR1に帰還される。したがって、シフトレジスタSR1~SR6がシフト動作をするとき、シフトレジスタSR6からは初期値データD1~D6および切り替え回路2の選択に応じた疑似ランダム信号が出力される。

また、5は暗号鍵設定手段であり、この暗号鍵設定手段5は、ハイレベルまたはローレベルを選

択する。以下、この秘密装置について説明する。

第2図は送信側のブロック図である。

同図において、20は疑似ランダム信号発生回路であり、この疑似ランダム信号発生回路20は、6段のシフトレジスタSR1~SR6の連続接続段1と、この連続接続段1の帰還路を選択する切り替え回路2とで構成される。

連続接続段1のシフトレジスタSR1~SR6のロードおよびシフト状態は、制御手段であるマイクロコンピュータ6からの制御信号S/Lによって制御される。制御信号S/Lがロード状態のとき、シフトレジスタSR1~SR6には、マイクロコンピュータ6からの初期値データD1~D6がロードされる。なお、これらシフトレジスタSR1~SR6はクロックCKに同期して動作するようにされる。

切り替え回路2は、種々のゲートおよびインバータで構成される。すなわち、アンドゲート21にはシフトレジスタSR5の出力信号が供給されると共に、マイクロコンピュータ6からの制御デ

ータD7が供給される。また、アンドゲート23にはシフトレジスタSR1の出力信号が供給されると共に、制御データD7がインバータ22を介して供給される。そして、これらアンドゲート21および23の出力信号がオアゲート24に供給される。したがって、制御データD7がハイレベルかローレベルかに応じて、オアゲート24からはシフトレジスタSR1またはSR5の出力信号が出力される。

また、3は例えばROM(リードオンリーメモリ)で構成され記憶回路であり、この記憶回路3には連続接続段1のシフトレジスタSR1~SR6に供給される初期値データD1~D6と、切り替え回路2に供給される制御データD7とが複数組記憶されている。

この場合、暗号鍵設定手段5で設定された暗号鍵に応じたアドレス信号がマイクロコンピュータ6より記憶回路3に供給され、対応する初期値データD1~D6および制御データD7が読み出される。そして、この初期値データD1~D6および制御データD7はマイクロコンピュータ6の端子P01~P07を介してシフトレジスタSR1~SR6および切り替え回路2に供給され、これにより疑似ランダム信号発生回路20が初期設定される。

BEST AVAILABLE COPY

また、マイクロコンピュータ6からのアドレス信号はパラレル/シリアル変換回路4でシリアル信号に変換されて出力される。

また、7はエクスクルーシブオアゲートで構成される暗号化回路であり、この暗号化回路7には、疑似ランダム信号発生回路20からの疑似ランダム信号と、データ発生手段(図示せず)からのシリアルデータ(例えば、音声データ)とが供給されて、シリアルデータは暗号化される。

また、8はデータ/制御信号切り替え回路であり、この切り替え回路8には変換回路4より出力されるアドレス信号、暗号化回路7より出力される暗号化データおよび同期信号発生回路9からの同期信号が供給される。そして、マイクロコンピュータ6の制御により、これらの信号はクロックCKに同期して切り替えられ、有線または無線の通信回線に出力される。第4図はその通信信号の構成例を示している。

このように、送信側では、暗号鍵設定手段5による暗号鍵の設定に応じて、データが暗号化され、

同期信号およびアドレス信号と共に、通信回線に出力される。

第3図は、受信側のブロック図である。この第3図において、第2図と対応する部分には同一符号を付して示している。

同図において、通信回線からの信号はデータ/制御信号切り替え回路8を介して同期信号検出回路12に供給され、この同期信号検出回路12で検出される同期信号(第4図参照)はマイクロコンピュータ6に供給される。

また、切り替え回路8には、マイクロコンピュータ6より同期信号に応じて制御信号およびクロックが供給される。そして、通信回線からの信号に含まれるアドレス信号は切り替え回路8よりシリアル/パラレル変換回路10でパラレル信号に変換されたのちマイクロコンピュータ6に供給される。そして、このアドレス信号はマイクロコンピュータ6より記憶回路3に供給され、対応する初期値データD1~D6および制御データD7が読み出される。そして、この初期値データD1~

D6および制御データD7はマイクロコンピュータ6の端子P01~P07を介してシフトレジスタSR1~SR6および切り替え回路2に供給される。これにより疑似ランダム信号発生回路20が初期設定される。

この場合、受信側および送信側の記憶回路3の記憶内容は同じであると共に、受信側および送信側の疑似ランダム信号発生回路20は同じ構成であるので、受信側の疑似ランダム信号発生回路20からは、送信側と同様の疑似ランダム信号が発生される。

また、11はエクスクルーシブオアゲートで構成される復号化回路である。この復号化回路11には、疑似ランダム信号発生回路20からの疑似ランダム信号と、切り替え回路8からの暗号化データとが供給され、暗号化データは復号化されて出力される。

このように第2図および第3図に示す秘話装置によれば、受信側で復号鍵を人力する必要はなく、送信側で暗号鍵を自由に更新することができる。

しかし、暗号鍵の設定はユーザーによって行なわれるものであり、ユーザーがその設定値を変更しない限り、疑似ランダム信号発生回路20からは常に同じ疑似ランダム信号が発生されて暗号化される。したがって、一度、第三者によって解読されると、通信の秘密を確保できなくなる。

そこで、この発明では、ユーザーを煩わせることなく、通信の秘密を十分に確保できる秘話装置を提供するものである。

〔課題を解決するための手段〕

この発明による秘話装置は以下のように構成される。すなわち、

送信側には、第1の疑似ランダム信号発生回路と、暗号鍵を設定する暗号鍵設定手段と、暗号鍵の設定値を変更する変換回路と、疑似ランダム信号発生回路の初期設定データを記憶した第1の記憶回路と、変換回路からの暗号鍵に対応したアドレス信号によって第1の記憶回路から初期設定データを読み出して第1の疑似ランダム信号発生回路を設定する第1の制御手段と、第1の疑似ラン

ダム信号発生回路の出力信号によって入力データを暗号化する暗号化回路とが備えられる。そして、暗号化回路の出力データおよびアドレス信号が送信される。

また、受信側には、第1の疑似ランダム信号発生回路と同じ構成の第2の疑似ランダム信号発生回路と、第1の記憶回路と同じ内容を記憶した第2の記憶回路と、受信したアドレス信号によって第2の記憶回路から初期設定データを読み出して第2の疑似ランダム信号発生回路を設定する第2の制御手段と、第2の疑似ランダム信号発生回路の出力信号によって受信したデータを復号化する復号化回路とが備えられる。

【作用】

上述構成においては、暗号鍵設定手段5からの暗号鍵の設定値を変更する変換回路17が設けられる。この変換回路17で暗号鍵は、例えば通信ごとに異なるように変更される。したがって、ユーザーを煩わせることなく暗号鍵の設定変更が行なわれ、通信の秘密を十分に確保できるようになる。

3図例と同様に構成される。

本例によれば、受信側で復号鍵を入力する必要はなく、送信側で暗号鍵を自由に変更することができる。そして、暗号鍵設定手段5からの暗号鍵は変換回路17で通信ごとに異なるように変更される。したがって、ユーザーを煩わせることなく、通信の秘密を十分に確保することができる。

なお、上述実施例においては、縦続接続段1のシフトレジスタの段数は6段とされたものであるが任意の段数とすることができる。また、シフトレジスタSR1に帰還する信号は、上述実施例に限定されることなく任意のシフトレジスタの出力とすることができる。

【発明の効果】

以上説明したように、この発明によれば、受信側で復号鍵を入力する必要はなく、送信側で暗号鍵を自由に変更することができると共に、暗号鍵設定手段からの暗号鍵は変換回路で、例えば通信ごとに異なるように変更されるので、ユーザーを煩わせることなく、通信の秘密を十分に確保する

る。

【実施例】

以下、第1図を参照しながら、この発明の一実施例について説明する。この第1図において、第2図と対応する部分には同一符号を付し、その詳細説明は省略する。

本例においては、暗号鍵設定手段5からの暗号鍵は演算回路で構成される暗号鍵変換回路17を介してマイクロコンピュータ6に供給される。変換回路17にはマイクロコンピュータ6より通信回数データのデータが供給され、暗号鍵設定手段5より供給される暗号鍵は通信ごとに異なるように変更される。

このように変更するための演算処理例としては、通信ごとに「1」を加算していくというような簡単なものから、PN発生回路によるスクランブル化、乗算、除算や各種演算による複雑なものまで考えられる。

本例は以上のように構成され、その他の部分は第2図例と同様に構成される。なお、受信側は第

ことができる。

4. 図面の簡単な説明

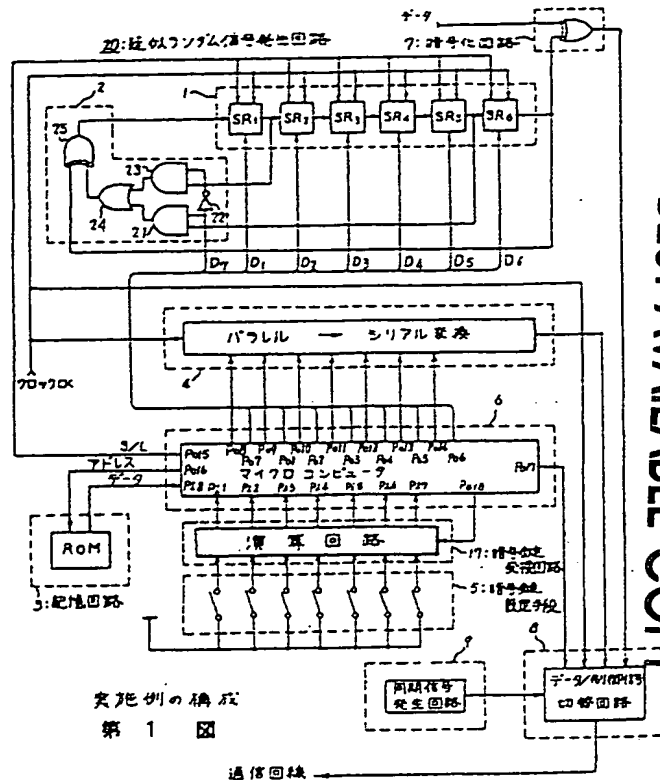
第1図はこの発明の一実施例を示すブロック図、第2図は秘密装置の送信側のブロック図、第3図は秘密装置の受信側のブロック図、第4図は通信信号の構成を示す図、第5図は従来の秘密装置のブロック図である。

- 3・・・記憶回路
- 4・・・パラレル／シリアル変換回路
- 5・・・暗号鍵設定手段
- 6・・・マイクロコンピュータ
- 7・・・暗号化回路
- 8・・・データ／制御信号切り替え回路
- 9・・・同期信号発生回路
- 10・・・シリアル／パラレル変換回路
- 11・・・復号化回路
- 12・・・同期信号検出回路
- 17・・・暗号鍵変換回路

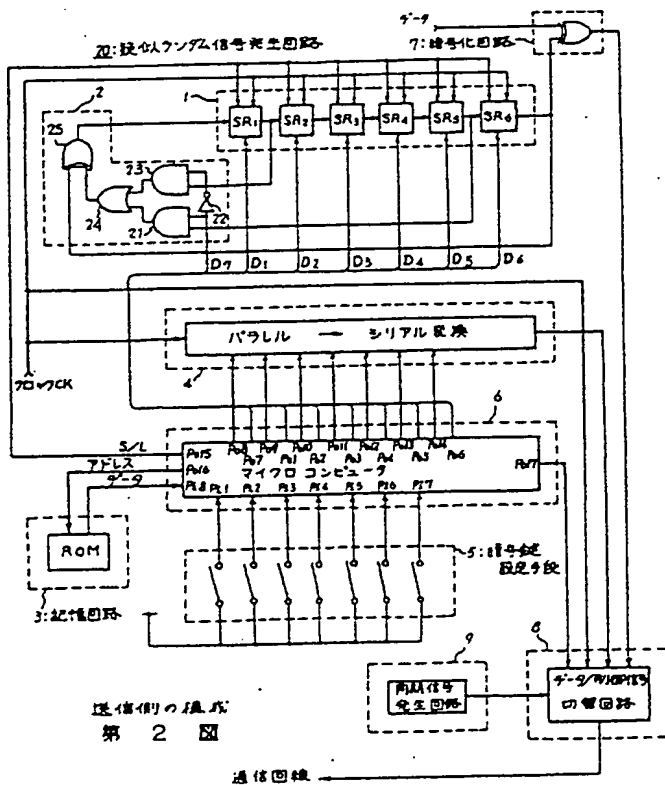
BEST AVAILABLE COPY

20... 疑似ランダム信号発生回路

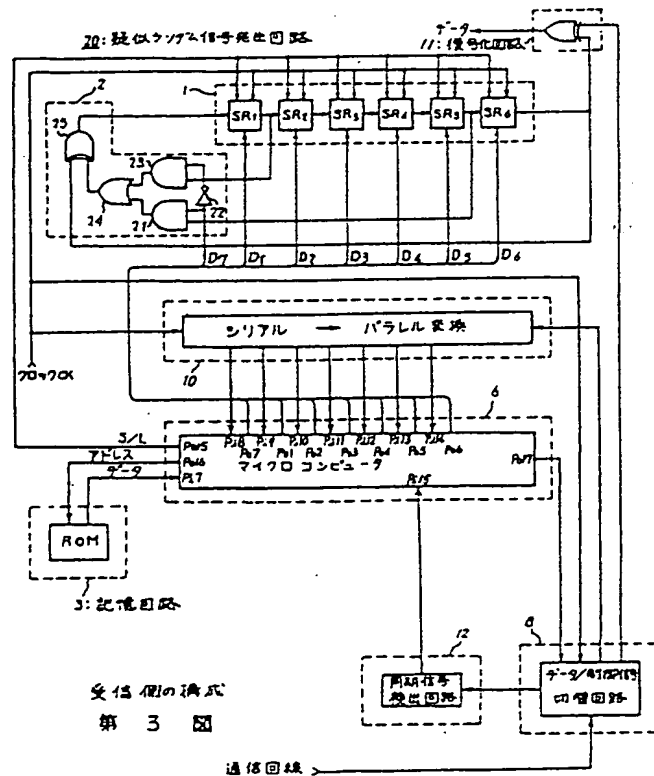
特許出願人 シ ャ ー プ 株式会社
代理人 弁理士 山 口 邦 夫



実施例の構成
第 1 図

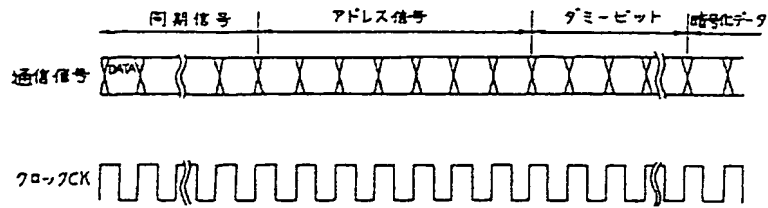


送信側の構成
第 2 図

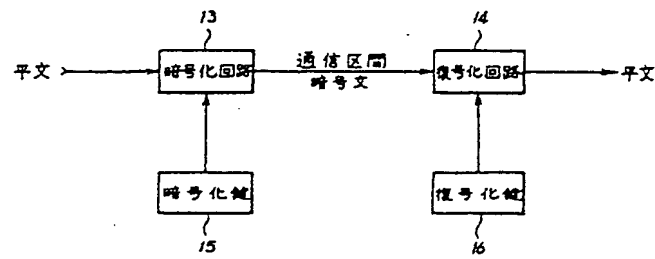


受信側の構成
第 3 図

BEST AVAILABLE COPY



通信信号の一例
第 4 図



従来例の構成図
第 5 図

BEST AVAILABLE COPY